



AF
Irw

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Brian C. Barnes, et al

Group Art Unit: 2137

Serial No.: 10/010,161

Examiner: Ali Abyaneh

Filed: 11/13/01

Atty. Dkt. No.: 2000.056700

For: Memory Management System And Method
Providing Linear Address Based Memory
Access Security

Client Docket: TT4087

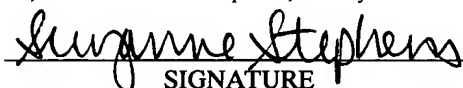
APPEAL BRIEF

Customer No.: 23720

MS APPEAL BRIEF – PATENTS
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING UNDER 37 C.F.R. § 1.8

I hereby certify that this paper or fee is being deposited with the United States Postal Service with sufficient postage as "FIRST CLASS MAIL" addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 12, 2006 by:


SIGNATURE

Sir:

Applicant hereby submits this Appeal Brief to the Board of Patent Appeals and Interferences in response to the final Office Action dated November 15, 2005. The fee for filing this Appeal Brief is \$500, and is attached hereto.

If the check is inadvertently omitted, or should any additional fees under 37 C.F.R. §§ 1.16 to 1.21 be required for any reason relating to the enclosed material, or should an overpayment be included herein, the Commissioner is authorized to deduct or credit said fees from or to Williams, Morgan & Amerson, P.C. Deposit Account No. 50-0786/2000.056700.

I. REAL PARTY IN INTEREST

The present application is owned by Advanced Micro Devices, Inc.

04/18/2006 TBESHAH1 00000043 500786 10010161

01 FC:1402 500.00 DA

II. RELATED APPEALS AND INTERFERENCES

Applicants, Applicants' representative(s), and the Assignee are not aware of any appeals, interferences, or judicial proceedings that are related to, may be affected by, might affect. or have a bearing on the Board's decision in this appeal.

III. STATUS OF THE CLAIMS

Claims 1-37 are pending in the case. Of these claims, claims 1-9, 11-13, 23, 32, and 36-37 were rejected under 35 U.S.C. § 102(b) by United States Letters Patent Maruyama, et al (U.S. Patent No. 6,052,763). Claims 10, 20, 22, 26, and 35 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Maruyama in view of admitted prior art.

IV. STATUS OF AMENDMENTS

No amendment has been filed which is not entered by the Examiner.

V. SUMMARY OF CLAIMED SUBJECT MATTER

In general, the present invention is directed to memory management systems and methods, and, more particularly, to memory management systems and methods that provide protection for data stored within a memory. There are six independent claims at issue in the current appeal: claims 1, 11, 12, 13, 23, and 32.

Independent claim 1 is generally directed to a memory management unit for managing a memory storing data arranged within a plurality of memory pages, the memory management unit. The memory unit further comprises a security check unit coupled to receive a linear address generated during execution of a current instruction, wherein the linear address has a corresponding physical address residing within a selected memory page, and wherein the

security check unit is configured to use the linear address to access at least one security attribute data structure located in the memory to obtain a security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the security attribute of the selected memory page, and to produce an output signal dependent upon a result of the comparison. The memory management unit further comprises a configuration to access the selected memory page dependent upon the output signal. By way of example only, at least portions of the invention are described at p. 9-24; Figures 4-9.

Independent claim 11 is generally directed to a central processing unit comprising an execution unit operably coupled to a memory, wherein the execution unit is configured to fetch instructions from the memory and to execute the instructions. The central processing unit further comprises a memory management unit (MMU) operably coupled to the memory and configured to manage the memory, wherein the MMU is configurable to manage the memory such that the memory stores data arranged within a plurality of memory pages, and wherein the MMU comprises a security check unit coupled to receive a linear address generated by the execution unit during execution of a current instruction, wherein the linear address has a corresponding physical address that resides within a selected memory page, and wherein the security check unit is configured to use the linear address to access at least one security attribute data structure located in the memory to obtain a security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the security attribute of selected memory page, and to produce an output signal dependent upon a result of the comparison. The MMU is configured to access the selected

memory page dependent upon the output signal. By way of example only, at least portions of the invention are described at p. 9-24; Figures 4-9.

Independent claim 12 is generally directed to a computer system, comprising a memory for storing data, wherein the data includes instructions and a central processing unit (CPU). The central processing unit comprises an execution unit operably coupled to the memory, wherein the execution unit is configured to fetch instructions from the memory and to execute the instructions; and a memory management unit (MMU) operably coupled to the memory and configured to manage the memory, wherein the MMU is configurable to manage the memory such that the memory stores the data arranged within a plurality of memory pages. The MMU comprises a security check unit coupled to receive a linear address generated by the execution unit during execution of a current instruction, wherein the linear address has a corresponding physical address residing within a selected memory page, and wherein the security check unit is configured to use the linear address to access at least one security attribute data structure located in the memory to obtain a security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the security attribute of selected memory page, and to produce an output signal dependent upon a result of the comparison. The MMU is configured to access the selected memory page dependent upon the output signal. By way of example only, at least portions of the invention are described at p. 9-24; Figures 4-9.

Independent claim 13 is generally directed to a memory management unit for managing a memory storing data arranged within a plurality of memory pages, the memory management unit comprising a paging unit coupled to the memory and to receive a linear address produced during execution of a current instruction, and configured to use the linear address to produce a physical

address within a selected memory page, wherein the paging unit is configured to use the linear address to access at least one paged memory data structure located in the memory to obtain security attributes of the selected memory page, and wherein the paging unit is configured to produce a fault signal dependent upon the security attributes of the selected memory page. The memory management unit comprises a security check unit coupled to receive the linear address produced during execution of the current instruction, and wherein the security check unit is configured to use the linear address to access at least one security attribute data structure located in the memory to obtain an additional security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the additional security attribute of selected memory page, and to produce an output signal dependent upon a result of the comparison. The memory management unit is configured to access the selected memory page dependent upon the output signal. By way of example only, at least portions of the invention are described at p. 9-24; Figures 4-9.

Independent claim 23 is generally directed to a memory management unit for managing a memory storing data arranged within a plurality of memory pages, the memory management unit comprising a paging unit coupled to the memory and to receive a linear address produced during execution of a current instruction residing within a first memory page, wherein the paging unit is configured to use the linear address to produce a physical address accessed by the current instruction, and wherein the physical address includes a base address of a selected memory page and an offset, and wherein the paging unit is configured to access at least one paged memory data structure located in the memory using the linear address to obtain the base address and security attributes of the selected memory page, and wherein the paging unit is configured to receive a security attribute of the instruction, and wherein the paging unit is configured to

produce a fault signal dependent upon the security attribute of the instruction and the security attributes of the selected memory page. The memory management unit comprises a security check unit coupled to receive the security attribute of the instruction, the security attributes of the selected memory page, and the linear address produced during execution of the current instruction, and wherein the security check unit is configured to use the linear address to access at least one security attribute data structure located in the memory to obtain an additional security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the additional security attribute of selected memory page, and to produce an output signal dependent upon a result of the comparison. The memory management unit is configured to access the selected memory page dependent upon the output signal. By way of example only, at least portions of the invention are described at p. 9-24; Figures 4-9.

Independent claim 32 is generally directed to a method for providing access security for a memory used to store data arranged within a plurality of memory pages, the method comprising receiving a linear address produced during execution of an instruction and a security attribute of the instruction, wherein the instruction resides in a first memory page and using the linear address to access at least one paged memory data structure located in the memory to obtain a base address of a selected memory page and security attributes of the selected memory page. The method further comprises combining the base address of the selected memory page with an offset to produce a physical address within the selected memory page if the security attribute of the instruction and the security attributes of the selected memory page indicate the access is authorized. The method further comprises generating a fault signal if the security attribute of the instruction and the security attributes of the selected memory page indicate the access is not

authorized. The method further comprises accessing at least one security attribute data structure located in the memory using the linear address produced during execution of the instruction to obtain an additional security attribute of the first memory page and an additional security attribute of the selected memory page. The method further comprises comparing a numerical value conveyed by an additional security attribute of the first memory page to a numerical value conveyed by the additional security attribute of selected memory page. The method further comprises accessing the selected memory page dependent upon a result of the comparing of the numerical values conveyed by the security attribute of the first memory page and the additional security attribute of selected memory page. By way of example only, at least portions of the invention are described at p. 9-24; Figures 4-9.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-37 are pending in the present application. The following issues are presented for review in the appeal: whether claims 1-9, 11-13, 23, 32, and 36-37 are anticipated by Maruyama and whether claims 10, 20, 22, 26, and 35 are rendered obvious over Maruyama in view of admitted prior art.

VII. ARGUMENT

Applicants respectfully submit that the Examiner erred in rejecting that claims 1-37. Therefore, Applicants respectfully request that the rejection of claims 1-9, 11-13, 23, 32, and 36-37 under the 35 U.S.C. §102(b), and claims 10, 20, 22, 26, and 35 under 35 U.S.C. § 103(a) be reversed.

A. Claims 1-9, 11-13, 23, 32, and 36-37 Are Allowable over Maruyama

1. Legal Standards

As the Board well knows, an anticipating reference by definition must disclose every limitation of the rejected claim in the same relationship to one another as set forth in the claim. *In re Bond*, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). **M.P.E.P. § 2131.**

Applicants respectfully assert that *Maruyama* does not teach, disclose or suggest using a linear address to access at least one security attribute data structure located in a memory to obtain a security attribute of a selected memory page in the memory, as called for by claim 1 of the present invention. The Examiner misinterprets the disclosure of *Maruyama*, which is directed to providing access security for a memory used to store data arranged within a plurality of memory pages in a protected virtual address mode (i.e., a protected mode) that uses both virtual memory and memory protection features. *See*; Abstract of *Maruyama*. This protects data stored in the memory so that software program or routine executing at the supervisor level may not access any portion of the memory or modify (i.e., write to) any portion of the memory that is not marked "read-only" (R/W=0). Thus, software program or routine cannot change any portion of the memory marked "read-only" to "read-write" (R/W=1), and then proceed to modify that portion of the memory. In contrast, the claims of the present invention are directed to techniques for managing a memory for storing data arranged within a plurality of memory pages. Claims 1, 11-13, 23, and 32 set forth, among other things, receiving a linear address generated during execution of a current instruction and using the linear address to access at least one security attribute data structure located in the memory, *i.e.* the memory that includes the plurality of memory pages, to obtain a security attribute of a selected memory page. Claims 1, 11-13, 23, and 32 also set forth comparing a numerical value conveyed by a security attribute of the current

instruction to a numerical value conveyed by the security attribute of the selected memory page and producing an output signal dependent upon a result of the comparison.

Maruyama is completely silent regarding using a linear address to access at least one security attribute data structure located in a memory to obtain a security attribute of a selected memory page in the memory. Instead, *Maruyama* teaches that unauthorized bus masters should not be permitted to access the dynamic random access memory (DRAM) 19 under certain circumstances. Thus, *Maruyama* fails to provide linear address based memory access security.

Claim 1 of the present invention is directed to accessing a security attribute data structure located in a memory to obtain a security attribute of a selected memory page in the memory, wherein *Maruyama* is directed to hosting the bus master identification table 24 in a different memory than the accessed memory pages. *Maruyama* does not disclose use of a common memory for the two as set forth above; it is merely directed to avoiding unintended modifying of a certain portion of the memory, which may be accessible to read only. In contrast, claim 1 of the present invention calls for using a linear address to access a security attribute data structure located in a memory to obtain a security attribute of a selected memory page in the memory. *Maruyama* clearly does not describe or suggest the use of the memory that includes the security attribute data structure and the selected memory page. Therefore, *Maruyama* does not anticipate use of the linear address to access one or more security attribute data structures located in a memory to obtain a security attribute of the selected memory page in the memory, as called for by claim 1 of the present invention.

Maruyama describes hosting the bus master identification table 24 in a EEPROM or a battery back-up RAM, and does not teach that the bus master identification table 24 should be hosted on the DRAM 19 that includes the accessed memory pages. See *Maruyama*, col. 5, ll. 33-

38 and Figure 1. In other words, *Maruyama* teaches hosting the bus master identifier table 24 in a different memory than the DRAM 19 that stores data, *i.e.*, a security attribute of a selected memory page, for which access requests are received. In particular, the bus master identifier table 24 is hosted in an EEPROM or battery backup RAM that is separate from the DRAM 19. See *Maruyama*, col. 5, ll. 34-35.

Thus, Applicants submit that *Maruyama* does not describe or suggest using a linear address to access at least one security attribute data structure located in a memory to obtain a security attribute of a selected memory page in the memory, *i.e.* the memory that includes the security attribute data structure and the selected memory page.

The Examiner acknowledges that Applicants argue that the cited reference “*Maruyama* does not teach that the bus master identification table 24 should be hosted on the DRAM 19 that includes the accessed memory page’ and “*Maruyama* does not describe or suggest using a linear address to access at least one security attribute data structure located in a memory to obtain a security attribute of a selected memory page in the memory.” To support his rationale for § 102 rejections, however, the Examiner instead cites column 5, lines 7-11 of *Maruyama* to state that *Maruyama* teaches the master ID table located on the memory unit. Furthermore, the Examiner asserts that *Maruyama* teaches accessing a lookup table and comparing a master ID with the entries in the lookup table (column 6, lines 47-55). Thus, according to the Examiner, since the master ID table is located on the memory unit and a lookup table is accessed for comparing a master ID, both the master ID table and the lookup table are described to be hosted on a same memory unit.

Maruyama describes a system bus interface unit 16 that receives memory access requests from a system bus 15 and sends access data to a dynamic random access memory (DRAM) 19.

The access addresses are stored in a decoder 21 while a bus master identification is sent to, and stored in, a register 22. The decoder 21 uses a flag bit to identify whether an access address is for a conventional address space or an atomic address space. If the access address is for an atomic address space, the register 22, comparator 23, and bus master identification table 24 determine if the requesting bus master has privileges for performing an atomic transaction. In particular, the comparator 24 accesses addresses from the register 22 and the bus master identification table 24. The comparator 24 then compares the accessed addresses. See *Maruyama*, col. 5, line 19 – col. 6, line 41 and Figure 1.

In the Final Office Action, the Examiner alleges that the bus master identification table 24 is located in the same memory as the accessed memory pages. Applicants respectfully disagree. *Maruyama* describes hosting the bus master identification table 24 in a EEPROM or a battery back-up RAM, and does not teach that the bus master identification table 24 should be hosted on the DRAM 19 that includes the accessed memory pages. See *Maruyama*, col. 5, ll. 33-38 and Figure 1. Thus, Applicants submit that *Maruyama* does not describe or suggest using a linear address to access at least one security attribute data structure located in a memory to obtain a security attribute of a selected memory page in the memory, *i.e.* the memory that includes the security attribute data structure and the selected memory page.

For at least the aforementioned reasons, it is respectfully submitted that the Examiner erred in rejecting independent claim 1. Therefore, claim 1 and claims dependent therefrom are in condition for allowance. Accordingly, the Examiner's rejections of claim 1 and its dependent claims should be reversed.

For at least the aforementioned reasons, Applicants respectfully submit that the present invention is not anticipated by *Maruyama* and request that the Examiner's rejections of claims 1-9, 11-13, 23, 32, and 36-37 under 35 U.S.C. 102(b) be reversed.

B. Claims 10, 20, 22, 26, and 35 are allowable over Maruyama in view of admitted prior art

2. Legal Standards

In the Office Action, claims 10, 20, 22, 26, and 35 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Maruyama* in view of admitted prior art. As the Board well knows, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991); M.P.E.P. § 2142. Moreover, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (CCPA 1974). If an independent claim is nonobvious under 35 U.S.C. § 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988); M.P.E.P. § 2143.03.

With respect to alleged obviousness, there must be something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination. *Panduit Corp.*

v. Dennison Mfg. Co., 810 F.2d 1561 (Fed. Cir. 1986). In fact, the absence of a suggestion to combine is dispositive in an obviousness determination. *Gambro Lundia AB v. Baxter Healthcare Corp.*, 110 F.3d 1573 (Fed. Cir. 1997). The mere fact that the prior art can be combined or modified does not make the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990); M.P.E.P. § 2143.01. The consistent criterion for determining obviousness is whether the prior art would have suggested to one of ordinary skill in the art that the process should be carried out and would have a reasonable likelihood of success, viewed in the light of the prior art. Both the suggestion and the expectation of success must be founded in the prior art, not in the Applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991); *In re O'Farrell*, 853 F.2d 894 (Fed. Cir. 1988); M.P.E.P. § 2142.

It is respectfully submitted that the pending claims are not obvious in view of *Maruyama* or the admitted prior art. To establish a *prima facie* case of obviousness, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (CCPA 1974). As discussed above, *Maruyama* fails to describe or suggest using a linear address to access at least one security attribute data structure located in a memory to obtain a security attribute of a selected memory page in the memory, as set forth in independent claims 1, 11-13, 23, and 32. The Examiner relies upon the admitted prior art to describe the use of a user/supervisor bit and a read/write bit. However, the admitted prior art fails to remedy the aforementioned fundamental deficiencies of the primary reference.

The cited references also fail to provide any suggestion or motivation to modify the prior art to arrive at Applicants' claimed invention. To the contrary, *Maruyama* teaches away from the present invention. In particular, *Maruyama* teaches that unauthorized bus masters should not

be permitted to access the dynamic random access memory 19 under certain circumstances. Accordingly, *Maruyama* teaches that the bus master identifier table 24 should be hosted in an EEPROM or battery backup RAM that is separate from the DRAM 19. See *Maruyama*, col. 5, ll. 34-35. *Maruyama* therefore teaches away from using a linear address to access at least one security attribute data structure located in a memory to obtain a security attribute of a selected memory page in the memory. It is by now well established that teaching away by the prior art constitutes *prima facie* evidence that the claimed invention is not obvious. See, *inter alia*, *In re Fine*, 5 U.S.P.Q.2d (BNA) 1596, 1599 (Fed. Cir. 1988); *In re Nielson*, 2 U.S.P.Q.2d (BNA) 1525, 1528 (Fed. Cir. 1987); *In re Hedges*, 228 U.S.P.Q. (BNA) 685, 687 (Fed. Cir. 1986).

For at least the aforementioned reasons, Applicants respectfully submit that the Examiner has failed to make a *prima facie* case that the present invention is obvious over *Maruyama* and the admitted prior art, either alone or in combination. Applicants request that the Examiner's rejections of claims 10, 20, 22, 26, and 35 under 35 U.S.C. 103(a) be reversed.

VIII. CLAIMS APPENDIX

The claims that are the subject of the present appeal – claims 1-37 – are set forth in the attached “Claims Appendix.”

IX. EVIDENCE APPENDIX

There is no separate Evidence Appendix for this appeal.

X. RELATING PROCEEDINGS APPENDIX

There is no Related Proceedings Appendix for this appeal.

XI. CONCLUSION

In view of the foregoing, Applicants respectfully submit that the Examiner's assertions that the inventions defined in claims 1-37 are anticipated and/or obviated by *Maruyama* are misplaced. It is respectfully submitted that the Examiner erred in not allowing all claims pending in the present application over the prior art of record. That is, Appellants respectfully submit that *Maruyama* does not disclose the entirety of the instant invention set forth in independent claims 1, 11, 12, 13, 23, and 18. Accordingly, Appellants respectfully request that the Board review and overturn the §102 and §103 rejections present in this case.

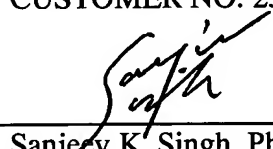
For at least the aforementioned reasons, Appellants respectfully request the Board reverse the Examiner's rejections of all the pending claims. The undersigned agent may be contacted at (713) 934-4089 with respect to any questions, comments or suggestions relating to this appeal.

Please date stamp and return the enclosed postcard to evidence receipt of this document.

Respectfully submitted,

WILLIAMS, MORGAN & AMERSON
CUSTOMER NO. 23720

Date: 04/13/06



Sanjeev K. Singh, Ph.D.

Rec. No. L0220

10333 Richmond, Suite 1100

Houston, Texas 77042

(713) 934-4089

(713) 934-7011 (facsimile)

AGENT FOR APPLICANTS



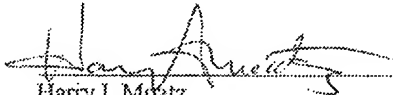
BEFORE THE OFFICE OF ENROLLMENT AND DISCIPLINE
UNITED STATE PATENT AND TRADEMARK OFFICE

LIMITED RECOGNITION UNDER 37 CFR § 11.9(b)

Dr. Sanjeev Kumar Singh is hereby given limited recognition under 37 CFR § 11.9(b) as an employee of Williams, Morgan & Amerson, P.C., to prepare and prosecute patent applications for clients of Williams, Morgan & Amerson, P.C. in which a member of Williams, Morgan & Amerson, P.C., is the attorney of record. This limited recognition shall expire on the date appearing below, or when whichever of the following events first occurs prior to the date appearing below: (i) Dr. Sanjeev Kumar Singh ceases to lawfully reside in the United States, (ii) Dr. Sanjeev Kumar Singh's employment with Williams, Morgan & Amerson, P.C. ceases or is terminated, or (iii) Dr. Sanjeev Kumar Singh ceases to remain or reside in the United States on an H-1B visa.

This document constitutes proof of such recognition. The original of this document is on file in the Office of Enrollment and Discipline of the U.S. Patent and Trademark Office.

Limited Recognition No. L0220
Expires: April 14, 2006


Harry L. Moatz
Director of Enrollment and Discipline

BEST AVAILABLE COPY

CLAIMS APPENDIX

1. A memory management unit for managing a memory storing data arranged within a plurality of memory pages, the memory management unit comprising:

a security check unit coupled to receive a linear address generated during execution of a current instruction, wherein the linear address has a corresponding physical address residing within a selected memory page, and wherein the security check unit is configured to use the linear address to access at least one security attribute data structure located in the memory to obtain a security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the security attribute of the selected memory page, and to produce an output signal dependent upon a result of the comparison; and

wherein the memory management unit is configured to access the selected memory page dependent upon the output signal.

2. The memory management unit as recited in claim 1, wherein the at least one security attribute data structure comprises a security attribute table directory and at least one security attribute table.

3. The memory management unit as recited in claim 2, wherein the security attribute table directory comprises a plurality of entries, and where each entry of the security attribute table

directory includes a present bit and a security attribute table base address field, and wherein the present bit indicates whether or not a security attribute table corresponding to the security attribute table directory entry is present in the memory, and wherein the security attribute table base address field is reserved for a base address of the security attribute table corresponding to the security attribute table directory entry.

4. The memory management unit as recited in claim 2, wherein the at least one security attribute table comprises a plurality of entries, and where each entry of the security attribute table includes a security context identification (SCID) field, and wherein the SCID field includes a plurality of bit positions, and wherein the bit positions form a binary representation of an SCID value, and wherein the SCID value is an integer value greater than or equal to 0, and wherein the SCID value indicates a security context level of a corresponding memory page.

5. The memory management unit as recited in claim 1, wherein the security attribute of the selected memory page comprises a security context identification (SCID) value, and wherein the SCID value is an integer value greater than or equal to 0 and indicates a security context level of the selected memory page.

6. The memory management unit as recited in claim 1, wherein the security attribute of the current instruction comprises a security context identification (SCID) value, and wherein the SCID value is an integer value greater than or equal to 0 and indicates a security context level of a memory page containing the current instruction.

7. The memory management unit as recited in claim 1, wherein the security check logic is configured to obtain the security attribute of the current instruction from the at least one security attribute data structure.

8. The memory management unit as recited in claim 1, wherein the output signal is a fault signal.

9. The memory management unit as recited in claim 1, wherein the security check unit is configured to receive a set of security attributes of the selected memory page in addition to the security attribute of selected memory page, and to produce the output signal dependent upon: (i) the result of the comparison of the numerical value conveyed by the security attribute of the current instruction to the numerical value conveyed by the security attribute of selected memory page, and (ii) the set of security attributes of the selected memory page.

10. The memory management unit as recited in claim 9, wherein the set of security attributes of the selected memory page comprise a user/supervisor (U/S) bit and a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates only read accesses are allowed to the selected memory page, and wherein R/W=1 indicates that both read and write accesses are allowed to the selected memory page.

11. A central processing unit, comprising:

an execution unit operably coupled to a memory, wherein the execution unit is configured to fetch instructions from the memory and to execute the instructions; and

a memory management unit (MMU) operably coupled to the memory and configured to manage the memory, wherein the MMU is configurable to manage the memory such that the memory stores data arranged within a plurality of memory pages, and wherein the MMU comprises:

a security check unit coupled to receive a linear address generated by the execution unit during execution of a current instruction, wherein the linear address has a corresponding physical address that resides within a selected memory page, and wherein the security check unit is configured to use the linear address to access at least one security attribute data structure located in the memory to obtain a security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the security attribute of selected memory page, and to produce an output signal dependent upon a result of the comparison; and

wherein the MMU is configured to access the selected memory page dependent upon the output signal.

12. A computer system, comprising:

a memory for storing data, wherein the data includes instructions;

a central processing unit (CPU), comprising:

an execution unit operably coupled to the memory, wherein the execution unit is configured to fetch instructions from the memory and to execute the instructions; and

a memory management unit (MMU) operably coupled to the memory and configured to manage the memory, wherein the MMU is configurable to manage the memory such that the memory stores the data arranged within a plurality of memory pages, and wherein the MMU comprises:

a security check unit coupled to receive a linear address generated by the execution unit during execution of a current instruction, wherein the linear address has a corresponding physical address residing within a selected memory page, and wherein the security check unit is configured to use the linear address to access at least one

security attribute data structure located in the memory to obtain a security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the security attribute of selected memory page, and to produce an output signal dependent upon a result of the comparison; and

wherein the MMU is configured to access the selected memory page dependent upon the output signal.

13. A memory management unit for managing a memory storing data arranged within a plurality of memory pages, the memory management unit comprising:

a paging unit coupled to the memory and to receive a linear address produced during execution of a current instruction, and configured to use the linear address to produce a physical address within a selected memory page, wherein the paging unit is configured to use the linear address to access at least one paged memory data structure located in the memory to obtain security attributes of the selected memory page, and wherein the paging unit is configured to produce a fault signal dependent upon the security attributes of the selected memory page; and

a security check unit coupled to receive the linear address produced during execution of the current instruction, and wherein the security check unit is configured to use

the linear address to access at least one security attribute data structure located in the memory to obtain an additional security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the additional security attribute of selected memory page, and to produce an output signal dependent upon a result of the comparison; and

wherein the memory management unit is configured to access the selected memory page dependent upon the output signal.

14. The memory management unit as recited in claim 13, wherein the at least one security attribute data structure comprises a security attribute table directory and at least one security attribute table.

15. The memory management unit as recited in claim 14, wherein the security attribute table directory comprises a plurality of entries, and where each entry of the security attribute table directory includes a present bit and a security attribute table base address field, and wherein the present bit indicates whether or not a security attribute table corresponding to the security attribute table directory entry is present in the memory, and wherein the security attribute table base address field is reserved for a base address of the security attribute table corresponding to the security attribute table directory entry.

16. The memory management unit as recited in claim 14, wherein the at least one security attribute table comprises a plurality of entries, and where each entry of the security attribute table includes a security context identification (SCID) field, and wherein the SCID field includes a plurality of bit positions, and wherein the bit positions form a binary representation of an SCID value, and wherein the SCID value is an integer value greater than or equal to 0, and wherein the SCID value indicates a security context level of a corresponding memory page.

17. The memory management unit as recited in claim 13, wherein the additional security attribute of the selected memory page comprises a security context identification (SCID) value, and wherein the SCID value is an integer value greater than or equal to 0 and indicates a security context level of the selected memory page.

18. The memory management unit as recited in claim 13, wherein the security attribute of the current instruction comprises a security context identification (SCID) value, and wherein the SCID value is an integer value greater than or equal to 0 and indicates a security context level of a memory page containing the current instruction.

19. The memory management unit as recited in claim 13, wherein the security check unit is coupled to receive a current privilege level (CPL) of a current task including the current instruction, and configured to produce the output signal dependent upon: (i) the result of the comparison of the numerical values conveyed by the security attribute of the current instruction and the security attribute of selected memory page, and (ii) the CPL of the current task including the current instruction.

20. The memory management unit as recited in claim 13, wherein the physical address within the selected memory page includes a base address and an offset, and wherein the paging unit is configured to obtain the base address from the at least one paged memory data structure.

21. The memory management unit as recited in claim 13, wherein the at least one paged memory data structure comprises a page directory and at least one page table as defined by the x86 processor architecture.

22. The memory management unit as recited in claim 13, wherein the security attributes of the selected memory page comprise a user/supervisor (U/S) bit and a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates only read accesses are allowed to the selected memory page, and wherein R/W=1 indicates that both read and write accesses are allowed to the selected memory page.

23. A memory management unit for managing a memory storing data arranged within a plurality of memory pages, the memory management unit comprising:

a paging unit coupled to the memory and to receive a linear address produced during execution of a current instruction residing within a first memory page, wherein

the paging unit is configured to use the linear address to produce a physical address accessed by the current instruction, and wherein the physical address includes a base address of a selected memory page and an offset, and wherein the paging unit is configured to access at least one paged memory data structure located in the memory using the linear address to obtain the base address and security attributes of the selected memory page, and wherein the paging unit is configured to receive a security attribute of the instruction, and wherein the paging unit is configured to produce a fault signal dependent upon the security attribute of the instruction and the security attributes of the selected memory page; and

a security check unit coupled to receive the security attribute of the instruction, the security attributes of the selected memory page, and the linear address produced during execution of the current instruction, and wherein the security check unit is configured to use the linear address to access at least one security attribute data structure located in the memory to obtain an additional security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the additional security attribute of selected memory page, and to produce an output signal dependent upon a result of the comparison; and

wherein the memory management unit is configured to access the selected memory page dependent upon the output signal.

24. The memory management unit as recited in claim 23, wherein the at least one paged memory data structure comprises a page directory and at least one page table as defined by the x86 processor architecture.

25. The memory management unit as recited in claim 23, wherein the security attribute of the current instruction comprises a current privilege level (CPL) of a task including the current instruction as defined by the x86 processor architecture.

26. The memory management unit as recited in claim 23, wherein the security attributes of the selected memory page comprise a user/supervisor (U/S) bit a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates only read accesses are allowed to the selected memory page, and wherein R/W=1 indicates that both read and write accesses are allowed to the selected memory page.

27. The memory management unit as recited in claim 23, wherein the additional security attribute of the selected memory page comprises a security context identification (SCID) value, and wherein the SCID value is an integer value greater than or equal to 0 and indicates a security context level of the selected memory page.

28. The memory management unit as recited in claim 23, wherein the security attribute of the current instruction comprises a security context identification (SCID) value, and wherein the SCID value is an integer value greater than or equal to 0 and indicates a security context level of the first memory page containing the current instruction.

29. The memory management unit as recited in claim 23, wherein the at least one security attribute data structure comprises a security attribute table directory and at least one security attribute table.

30. The memory management unit as recited in claim 29, wherein the security attribute table directory comprises a plurality of entries, and where each entry of the security attribute table directory includes a present bit and a security attribute table base address field, and wherein the present bit indicates whether or not a security attribute table corresponding to the security attribute table directory entry is present in the memory, and wherein the security attribute table base address field is reserved for a base address of the security attribute table corresponding to the security attribute table directory entry.

31. The memory management unit as recited in claim 29, wherein the at least one security attribute table comprises a plurality of entries, and where each entry of the security attribute table includes security context identification (SCID) field, and wherein the SCID field includes a plurality of bit positions, and wherein the bit positions form a binary representation of an SCID value, and wherein the SCID value is an integer value greater than or equal to 0, and wherein the SCID value indicates a security context level of a corresponding memory page.

32. A method for providing access security for a memory used to store data arranged within a plurality of memory pages, the method comprising:

receiving a linear address produced during execution of an instruction and a security attribute of the instruction, wherein the instruction resides in a first memory page;

using the linear address to access at least one paged memory data structure located in the memory to obtain a base address of a selected memory page and security attributes of the selected memory page;

combining the base address of the selected memory page with an offset to produce a physical address within the selected memory page if the security attribute of the instruction and the security attributes of the selected memory page indicate the access is authorized;

generating a fault signal if the security attribute of the instruction and the security attributes of the selected memory page indicate the access is not authorized;

accessing at least one security attribute data structure located in the memory using the linear address produced during execution of the instruction to obtain an additional security attribute of the first memory page and an additional security attribute of the selected memory page;

comparing a numerical value conveyed by an additional security attribute of the first memory page to a numerical value conveyed by the additional security attribute of selected memory page; and

accessing the selected memory page dependent upon a result of the comparing of the numerical values conveyed by the security attribute of the first memory page and the additional security attribute of selected memory page.

33. The method as recited in claim 32, wherein the receiving comprises:

receiving a linear address produced during execution of an instruction and a security attribute of the instruction, wherein the instruction resides in a first memory page, and wherein the security attribute of the instruction comprises a current privilege level (CPL) of a task including the instruction as defined by the x86 processor architecture.

34. The method as recited in claim 32, wherein the using comprises:

using the linear address to access at least one paged memory data structure located in the memory to obtain a base address of a selected memory page and security attributes of the selected memory page, wherein the at least one paged memory

data structure comprises a page directory and at least one page table as defined by the x86 processor architecture.

35. The method as recited in claim 31, wherein the combining comprises:

combining the base address of the selected memory page with an offset to produce a physical address within the selected memory page if the security attribute of the instruction and the security attributes of the selected memory page indicate the access is authorized, wherein the security attributes of the selected memory page comprise a user/supervisor (U/S) bit a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates only read accesses are allowed to the selected memory page, and wherein R/W=1 indicates that both read and write accesses are allowed to the selected memory page.

36. The method as recited in claim 31, wherein the generating comprises:

generating a fault signal if the security attribute of the instruction and the security attributes of the selected memory page indicate the access is not authorized,

wherein the fault signal is a general protection fault (GPF) signal as defined by the x86 processor architecture.

37. The method as recited in claim 31, wherein the accessing comprises:

accessing at least one security attribute data structure located in the memory using the linear address produced during execution of the instruction to obtain an additional security attribute of the first memory page and an additional security attribute of the selected memory page, wherein the at least one security attribute data structure comprises a security attribute table directory and at least one security attribute table, and wherein the additional security attribute of the first memory page comprises a security context identification (SCID) value of the first memory page, and wherein the SCID value of the first memory page is an integer value greater than or equal to 0 and indicates a security context level of the first memory page, and wherein the additional security attribute of the selected memory page comprises a security context identification (SCID) value of the selected memory page, and wherein the SCID value of the selected memory page is an integer value greater than or equal to 0 and indicates a security context level of the selected memory page.